Claims

1.   A computer-implemented method for securely transmitting an information

package from a sender to an addressee via a network, the method comprising a

server system performing the steps of:

5   receiving a delivery from the sender, the delivery comprising:

            the information package encrypted with a package encryption key; and

            a package decryption key encrypted with an escrow key;

        storing the delivery in escrow for the addressee;

        sending to the addressee a notification of the delivery;

10   and

        in response to receiving an acknowledgement from the addressee:

            obtaining a new public key of the addressee;

            decrypting the package decryption key;

            encrypting the package decryption key with the addressee's new public

15   key; and

            transmitting to the addressee the information package encrypted with the

                package encryption key and the package decryption key encrypted

                with the addressee's new public key.

2.   The method of claim 1 further comprising the server system performing the steps

20   of:

        receiving a request from the sender for a public key of the addressee;

        determining whether the addressee has a public key; and

        in response to not finding a public key of the addressee:

            transmitting the escrow key to the sender.

3.   The method of claim 2 wherein the step of determining whether the addressee has a public key comprises the sub-step of:

checking a public key database for a public key of the addressee.

4.   The method of claim 1 further comprising the server system performing the steps of:

in response to the sender searching a public key database for a public key of the addressee and not finding a public key of the addressee:

receiving a request from the sender for the escrow key; and

transmitting the escrow key to the sender.

5.   The method of claim 1, further comprising the server system performing the steps of:

issuing the new public key to the addressee; and

storing the addressee's new public key in a public key database.

6.   The method of claim 1, wherein the escrow key is one of a group comprising a symmetric key and an asymmetric key.

7.   The method of claim 1, wherein the notification is one of a group comprising an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification.

8.   The method of claim 1 further comprising the server system performing the steps of:

receiving from the sender a digest of one from a group comprising:

the information package;

the information package encrypted with the package encryption key; and

the information package encrypted with the package encryption key and

the package decryption key encrypted with the escrow key;

and

in response to receiving the acknowledgement from the addressee:

5   transmitting the digest to the addressee.

9.   The method of claim 8, wherein the digest is encrypted by a private key of the

sender.

10.   The method of claim 1, wherein the acknowledgement from the addressee

further comprises the step of authenticating the identity of the addressee.

10   11.   A system for securely transmitting an information package from a sender to an

addressee via a network, the system comprising:

a storage module, comprising a computer-readable storage medium, for

receiving, and storing in escrow, a delivery from the sender, said delivery

comprising:

15   a package decryption key encrypted with an escrow key, and

the information package encrypted with a package encryption key;

a notification module coupled to the storage module, for sending a notification to

the addressee via the network;

a key registration module coupled to the notification module for, in response to

20   receiving an acknowledgement from the addressee, receiving a new

public key of the addressee; and

a transmission module coupled to the storage module, for decrypting the

package decryption key and re-encrypting the package decryption key

with the new public key of the addressee, and for transmitting to the

25   addressee the information package encrypted with the package

encryption key and the package decryption key encrypted with the addressee's new public key.

12. The system of claim 11 further comprising:

a directory interface coupled to the storage module for checking, in response to

5   receiving a request from the sender for a public key of the addressee, a

public key database for the public key of the addressee; and

an escrow key manager coupled to the directory interface for providing, in

response to the directory interface failing to obtain a public key of the

addressee from the public key database, an escrow key for encrypting the

10   package decryption key.

13. The system of claim 11, wherein the key registration module also stores the addressee's new public key in a public key database.

14. The system of claim 11, further comprising:

a public key database coupled to the directory interface for storing a public key

15   of at least one addressee.

15. The system of claim 11, wherein the escrow key comprises one from a group comprising a symmetric key and an asymmetric key.

16. The system of claim 11, wherein the notification is one of a group comprising an e-mail notification, a desktop notification, a voice notification, a pager notification,

20   and a facsimile notification.

17. The system of claim 11 further comprising:

an authentication module coupled to the notification module for authenticating

the addressee prior to transmitting the information package encrypted

with the package encryption key and the package decryption key encrypted with the addressee's new public key.

18.   A computer-readable medium comprising computer program code for securely transmitting an information package from a sender to an addressee via a network,

5   the computer program code adapted to perform the steps of:

receiving a delivery from the sender, the delivery comprising:

the information package encrypted with a package encryption key; and

a package decryption key encrypted with an escrow key;

storing the delivery in escrow for the addressee;

10   sending to the addressee a notification of the delivery;

and

in response to receiving an acknowledgement from the addressee:

obtaining a new public key of the addressee;

decrypting the package decryption key;

15   encrypting the package decryption key with the addressee's new public

key; and

transmitting to the addressee the information package encrypted with the

package encryption key and the package decryption key encrypted

with the addressee's new public key.

20   19.   The computer-readable medium of claim 18 further comprising program code adapted to perform the steps of:

receiving a request from the sender for a public key of the addressee;

determining whether the addressee has a public key; and

in response to not obtaining a public key of the addressee:

25   transmitting the escrow key to the sender.

20735/05503/DOCS/1149971.4

20.	The computer-readable medium of claim 19, further comprising program code adapted to perform the step of:

checking a public key database for the public key of the addressee.

21.	The computer-readable medium of claim 18, further comprising program code adapted to perform the steps of:

in response to the sender searching a public key database for a public key of the addressee and not obtaining said public key:

receiving a request from the sender for the escrow key; and

transmitting the escrow key to the sender.

22.	The computer-readable medium of claim 18, further comprising program code adapted to perform the steps of:

issuing the new public key to the addressee; and

storing the addressee's new public key in a public key database.

23.	The computer-readable medium of claim 18, wherein the notification is one of a group comprising an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification.

24.	The computer-readable medium of claim 18, further comprising program code adapted to perform the steps of:

receiving from the sender a digest of one from a group comprising:

the information package;

the information package encrypted with the package encryption key; and

the information package encrypted with the package encryption key and

the package decryption key encrypted with the escrow key;

and

in response to receiving the acknowledgement from the addressee:

35	20735/05503/DOCS/1149971.4

transmitting the digest to the addressee.

25.   The method of claim 23, wherein the digest is encrypted by a private key of the sender.

26.   The computer-readable medium of claim 18, further comprising program code adapted to perform the step of:

authenticating the addressee prior to transmitting the information package encrypted with the package encryption key and the package encryption key encrypted with the addressee's new public key.

36   20735/05503/DOCS/1149971.4